

## —政策関連—

**みずほ中国 ビジネス・エクスプレス**  
( 第 514 号 )**中国、デジタル経済促進に向けた情報管理関連の法整備を推進**  
(外資系企業も慎重な対応が必要に)

平素より格別のご高配を賜り誠にありがとうございます。

中国政府当局の主な政策動向等に関する最新情報をお知らせ致します。

近年、中国当局は政府や企業が扱うデータの管理体系の整備に向けて法整備を推進しており、今月初めに中国全人代（国会に相当）は『データ安全法（草案）』を公表し、意見募集を開始しました。

これまで 2017 年施行の『インターネット安全法』や、同法の行政規則である『サイバーセキュリティ審査弁法』（2020 年 6 月施行）に加え、新たに近時、専門家による草案作成中といわれる『個人情報保護法』も含め、一連の法令規則は中国でデータ管理の法的枠組みの柱となろうとしています。

今般の『データ安全法（草案）』については、中国のデータの取り扱いにかかわる初めての包括的な法律となり、データ取引管理制度や国家の安全の影響を審査する制度を構築していくとされています。その対象データについては、現草案では電子データに加えて、非電子データも適用対象となっています。主な注目点については下表をご参照ください。

**『データ安全法（草案）』の注目点（抜粋）**

カテゴリー	主な内容
域外適用	✓ 域外の組織、個人がデータ活動を展開し、中国の国の安全、公共の利益または公民、組織の合法的な権益に損害を与えた場合、法律に基づいて責任を追及する（第 2 条）
監督管理の役割分担	✓ 工業、電信、自然資源、衛生、金融等の業界主管部門はそれぞれの業界のデータに対する監督管理を行う。国のインターネット情報管理部門は監督管理の統括を行う（第 7 条）
デジタル経済発展計画提起	✓ 国はビッグデータ戦略を実施。省レベル以上の政府はデジタル経済発展計画を制定、当該政府の国民経済と社会発展計画に組み入れ（第 13 条）
取引市場の育成	✓ 国はデータ取引管理制度を構築、健全化し、データ取引市場を育成する（第 17 条）
データ統制強化	✓ データの改ざんや漏洩、不正利用などが発生した場合の危害の程度に応じ、政府がデータを国家安保の観点からランク付けし、重点保護するデータ目録などを作る（第 19 条）
規制対象データに輸出制限	✓ 国は、国際的義務の履行や国の安全保障の維持に関連する規制対象品目に該当するデータについて、法律に基づいて輸出規制を実施する（第 23 条）
制裁に対等の対抗措置	✓ 外国政府などが投資や貿易分野のデータ利用などで中国に差別的な制限・禁止措置をとれば、相応の対抗措置を講じられる（第 24 条）
外国機関へのデータ提供に規制	✓ 国外の法執行機関が、中国国内に保存されたデータを調査する際は、関連組織や個人が関連管理機関に報告し、許可を得た後、提供しなければならない（第 33 条）

（『データ安全法（草案）』に基づき、中国アドバイザー一部作成）

外資系企業にとっては、将来の業務運営やデータ利用に支障が出ないように、草案が今後どう修正されるのか、またこれから策定される具体的な関連規則などをフォローし慎重に対応する必要があるかと思われまます。

草案は今後、募集した意見を踏まえ、改正されるところが少なくないかもしれないため、現時点では、その内容を逐次解説するというよりは、草案から読み取れる当局の方針や制度・取り組みの方向感の一考に値するのではないかと思われまます。

引き続き、最新情報の都度、このビジネス・エクスプレス等でお伝えするように致します。

## 【ご参考】（過去の経緯等）

### □ サイバーセキュリティーについて

2019年公布の『インターネット安全法』（別名：サイバーセキュリティー法）は顧客データを海外に持ち出す際に当局の審査を義務付けるほか、重要情報インフラの運営者が、ネットワーク製品・サービスを調達する場合に、国家の安全に影響を及ぼす可能性がある場合、国が実施するサイバーセキュリティー審査に合格しなければならないと規定しています。また、2020年6月公布の『サイバーセキュリティー審査弁法』は、サイバーセキュリティー審査の申請手続などを詳しく定め、通信や金融などの公共インフラ運営企業がIT（情報技術）機器を調達する際に当局による安全保障上の審査を受けることを義務付けています。

### □ 個人情報保護について

過去、国家インターネット情報弁公室は2019年5月に『データ安全管理弁法』の意見募集案を発表し、同年6月28日まで意見募集を行っていました。この意見募集案では、「重要データには一般的に企業の生産管理・内部管理情報、個人情報等は含まれない」という内容や、2020年4月公布の『情報安全技術個人情報安全規範』<sup>1</sup>等に基づき、個人情報の収集、取り扱い等に関する指針などもありました。また、個人情報保護について、『データ安全管理弁法』は今年5月に可決された民法典や、策定中の『個人情報保護法』と相互補完的なものとみられていますが、現時点では『データ安全管理弁法』の正式版は未だに公布されていないため、これら法令規則の動きに引き続き注視する必要があります。

### □ 情報インフラの保護について

情報インフラの保護について、2008年以降公布の『情報安全技術 情報システム安全等級保護分類ガイド』（GB/T 22240-2008）は、侵害対象によって情報システムの侵害レベルの認定基準を定めています。また、2019年12月から実施された『信息安全技術 インターネット安全等級保護基本要求』、『情報安全技術 インターネット安全等級保護評価要求』などは情報インフラに対する等級保護制度について明記しています。

\*

『データ安全法（草案）』の詳細については、5ページからの日本語（仮訳）および11ページからの中国語原文をご参照ください。

<sup>1</sup> 2020年版の『情報安全技術 個人情報安全規範』（GB/T 35273-2020）は2020年10月1日から発効、2018年5月から実施された『情報安全技術 個人情報安全規範』（GB/T 35273-2017）を改定したものです。関連内容は下記のアクセスをご参照ください。

⇒<http://www.ahstu.edu.cn/wlzx/info/1011/1478.htm>

## —当局政策関連—

年初以来、中央政府は新型コロナウイルスの感染の影響を最小限に抑えるために各種支援策を発表しております。地方政府も、中央政府の方針に基づき、現地の状況に合わせた関連措置を引き続き打ち出しており、中国全土における操業再開の更なる拡大や、映画館、スポーツイベントの再開などの動きが見られております。

ここでは新型コロナウイルス関連政策に限らず、当局政策の中で、直近に公布されたその他の主な政策をお知らせ致します。

### 【政府当局の主な政策動向】

政府機関	政策名（公布日）	備考（趣旨）
<b>国務院</b>	<p>ビジネス環境の更なる最適化による市場主体へのサポート強化に関する国務院弁公庁の実施意見 国弁発〔2020〕24号 (2020. 7. 21)</p> <p>国务院办公厅关于进一步优化营商环境更好服务市场主体的实施意见 国办发〔2020〕24号 <a href="http://www.gov.cn/zhengce/content/2020-07/21/content_5528615.htm">http://www.gov.cn/zhengce/content/2020-07/21/content_5528615.htm</a></p>	<ul style="list-style-type: none"> <li>➢ 工事建設、教育、医療、スポーツなどの分野において、関連部門や地方政府は市場参入に係る企業の資質、資金などの面で設けている非合理的な条件を集約的に整理する</li> <li>➢ 輸出入通関の効率を高める。企業が輸出入貨物の事前通関申告をすれば、貨物が税関に到着した後、直ちに検査と通関手続きを行うことが可能となる</li> <li>➢ 輸出入に係る証明手続きは原則として「単一窓口」で一括対応される。企業によるオンラインでの料金支払いや、証明書印刷を実現する</li> <li>➢ 貿易企業による輸出製品の国内販売を支持し、従来の国内認証から貿易企業の自己声明等の方式への変更を推進する。認証標準につき国内標準を下回らない国際認証を取得した製品の場合、貿易企業が国内標準に合致するという承諾書を提出した後、直接国内市場で販売することを認める</li> <li>➢ 条件が揃った特定の道路及びニーズがある空港、港湾、園区等の区域においてインテリジェントコネクテッドビークル（ICV）の応用示範を模索する</li> <li>➢ 企業設立関連手続きの全面的なオンライン実施を推進する。税務、人的資源などのサービス分野において、営業許可書や印鑑の電子化を実現する。「一つの産業で、一つの許可書」改革を推進し、単独の産業における複数の許可書を一つに集約し、異なる地域での許可書情報の共有などを実現する</li> <li>➢ 2020年末までに、基本的に増値税専用領収書の電子化、主な税金関連手続きのオンライン化を実現する。増値税など税金優遇の申請プロセスを簡素化する。税務、税関、人民銀行など関連部門のデータ共有を強化し、輸出税還付の所要時間を短縮させる</li> <li>➢ 2020年末までに商標登録の平均審査期間を4カ月以内に短縮する</li> <li>➢ 商業銀行が売掛金、生産設備、製品、車両、船舶、知的財産権等の動産及び無形資産を担保とした中小企業向け融資を支持することを奨励・誘導する。担保提供者の名称別索引があるデータベースを構築し、担保物の登記状態情報に対する調査、改正、若しくは抹消のオンライン実施を実現する</li> </ul>

政府機関	政策名（公布日）	備考（趣旨）
中国銀行保険監督管理委員会	<p>信用保証会社の非現場監督管理規程に関する中国銀保監会の通知 (2020. 7. 24)</p> <p>中国银保监会关于印发融资担保公司非现场监管规程的通知 <a href="http://www.cbirc.gov.cn/cn/view/pages/ItemDetail.html?docId=918140&amp;itemId=928&amp;generalType=0">http://www.cbirc.gov.cn/cn/view/pages/ItemDetail.html?docId=918140&amp;itemId=928&amp;generalType=0</a></p>	<ul style="list-style-type: none"> <li>➤ 地方政府の金融監督管理部門（以下、監督管理部門）は非現場監督管理の主担当として、域内の信用保証会社及びその拠点に対する非現場監督管理作業を実施する</li> <li>➤ 銀保監会の省級出先機関（以下、銀保監局）は管轄下の銀行業金融機関（法人及び拠点を含む）と信用保証会社との連携状況に対するモニタリングを行う</li> <li>➤ 非現場監督管理は、ビッグデータ等のIT技術を活用しリスクをリアルタイムで監視しなければならない</li> <li>➤ 信用保証会社に対する非現場監督管理は、情報の収集と確認、リスクの監視と評価、情報の報告と利用、監督管理措置の実施の4部分から構成される</li> <li>➤ 監督管理部門と銀保監局は作業の必要に応じ、信用保証会社と銀行業金融機関のデータマネジメント及び指標の正確性に対しヒアリング、面談、特別評価、現地訪問と立入検査等を行うことが可能である</li> <li>➤ 監督管理部門と銀保監局は情報共有と定期的なコミュニケーションを強化し、監督管理に総力を上げなければならない</li> <li>➤ 本規程は2020年9月1日より施行する</li> </ul>
北京市政府	<p>演出空間、娯楽施設、インターネットカフェによる秩序ある営業活動の再開に関する北京市文化・旅行局の通知 京文旅発〔2020〕239号 (2020. 7. 21)</p> <p>北京市文化和旅游局关于演出场所、娱乐场所、互联网上网服务营业场所有序恢复经营活动的通知 京文旅发〔2020〕239号 <a href="http://www.beijing.gov.cn/zhengce/zhengcefagui/202007/t20200722_1954564.html">http://www.beijing.gov.cn/zhengce/zhengcefagui/202007/t20200722_1954564.html</a></p>	<ul style="list-style-type: none"> <li>➤ 所在地の区政府により認可を経て、演出空間や、娯楽施設、インターネットカフェの秩序ある営業活動を再開する             <ul style="list-style-type: none"> <li>● 劇場等の演出空間：観客数は観客席数の3割を超えてはならない。間隔を置き着席し、1メートルのソーシャルディスタンス（社会的距離）を保つ。複数の劇場を有する演出空間の場合、営業再開できる劇場は1つに限定される。中・大型営業性公演・イベント活動や、渉外営業性公演・イベント活動（出演者・スタッフが既に中国本土に滞在する場合を除く）の再開を見合わせる</li> <li>● 娯楽施設：ディスコ、カラオケ店等の入場者数は定員の5割を超えてはならない。ゲームセンターの入場者数は定員の5割を超えてはならず、客の1回当たり滞在時間を2時間までに制限する</li> <li>● ネットカフェ：入場者数は定員の5割を超えてはならず、客の1回当たり滞在時間を2時間までに制限する</li> </ul> </li> <li>➤ 警戒レベルが「中・高リスク」である地域については上記場所の営業再開を見合わせる</li> </ul>

（各公開資料に基づき、中国アドバイザー一部作成）

## 中華人民共和国データ安全法(草案)

### 目録

- 第一章 総則
- 第二章 データの安全と発展
- 第三章 データ安全制度
- 第四章 データの安全保護義務
- 第五章 政務関連データの安全と公開
- 第六章 法的責任
- 第七章 附則

### 第一章 総則

第一条 データの安全を保障し、データの開発利用を促進し、公民、組織の合法的な権益を保護し、国の主権、安全と発展の利益を守るために、本法を制定する。

第二条 中華人民共和国国内において展開するデータ活動につき、本法を適用する。

中華人民共和国国外の組織、個人がデータ活動を展開し、中華人民共和国の国の安全、公共の利益または公民、組織の合法的な権益に損害を与えた場合、法律に基づいて責任を追及する。

第三条 本法でいうデータとは、電子的形式または非電子的形式のいずれかで情報が記録されたものをいう。

データ活動とは、データの収集、保存、加工、使用、提供、取引、公開などの行為を指す。

データセキュリティとは、必要な措置を講じることで、データが効果的に保護され、合法的に利用され、継続的に安全な状態が維持される能力を指す。

第四条 データの安全を維持するにあたり、国全体の安全観を堅持し、健全なデータセキュリティガバナンスシステムを確立し、データの安全保障能力を高めなければならない。

第五条 国は公民、組織とデータに関連する権益を保護し、データが法に基づいて合理的かつ有効に利用されることを奨励し、データの法に基づいた秩序ある且つ自由な流通を保障し、データをカギとするデジタル経済の発展を促進し、人民の福祉を増進する。

第六条 中央国家安全指導機構はデータ安全業務の方策と統一的協調の責任を負い、国のデータ安全戦略



及び関連重大方針政策の研究、策定、指導、実施をする。

第七条 各地区、各部門は本地区、本部門の業務中に発生し、とりまとめ、加工したデータ及びデータの安全に対して主体的責任を負う。

工業、電信、自然資源、衛生・健康、教育、国防科学技術工業、金融業などの業界主管部門はそれぞれの業界、それぞれの分野のデータに対する安全・監督・管理の職責を担う。

公安機関、国家安全機関などは本法及び関連法律、行政法規の規定により、各自の職責の範囲内においてデータの安全・監督・管理につき職責を担う。

国のネットワークセキュリティ・情報化関連部門は本法と関連法律、行政法規の規定に基づいて、ネットワークデータセキュリティと関連監督・管理業務の統一的な協調を担う。

第八条 データ活動を展開する際は、法律、行政法規を遵守し、社会の公衆道徳と倫理を尊重し、商業道徳を遵守し、誠実で信用を守り、データの安全保護義務を履行し、社会的責任を負い、国の安全、公共の利益に危害を与えず、公民、組織の合法的な権益を損害してはならない。

第九条 国はデータ安全協同管理体系を構築、かつ健全化し、関連部門、業界団体、企業、個人などが共にデータの安全保護業務に参加することを推進し、全社会が共にデータの安全を維持し、発展を促進する良好な環境を形成する。

第十条 国は積極的にデータ分野での国際交流と協力を展開し、データセキュリティ関連の国際ルールと標準の制定に参加し、データの国境を越えた安全、自由な流通を促進する。

第十一条 いかなる組織、個人も本法に違反する行為に対して関連主管部門にクレーム、通報する権利を有する。クレーム・通報を受けた部門は速やかに法律に基づいて処理すべきである。

## 第二章 データの安全と発展

第十二条 国はデータ安全の維持とデータ開発利用の推進を共に重んじ、データ開発利用と産業発展を通じデータの安全を促進し、データの安全を以ってデータの開発利用及び産業発展を保障する。

第十三条 国はビッグデータ戦略を実施し、データインフラの建設を推進し、各業界、各分野におけるデータの革新的な応用を奨励、支援し、デジタル経済の発展を促進する。

省レベル以上の人民政府はデジタル経済発展計画を制定し、当該レベル国民経済と社会発展計画に組み入れなければならない。

第十四条 国はデータ開発利用技術の基礎研究を強化し、データの開発利用と安全などの分野における技術の普及とビジネスイノベーションをサポートし、データの開発利用とデータセキュリティ製品及び産業体系を育成、発展させる。

第十五条 国はデータ開発利用技術とデータ安全標準体系の構築を推進する。国务院標準化行政主管部門と国务院関連部門は各自の職責に基づき、データ開発利用技術、製品及びデータの安全に関連する標準を制定し、適時改訂する。国は企業、研究機関、大学・大学院、関連業界組織などが基準の制定に参与するようサポートする。

第十六条 国はデータの安全に係る検査、評価、認証などサービスの発展を促進し、データの安全に係る検査、評価、認証などの専門機構が法律に基づいてサービス活動の展開をサポートする。

第十七条 国はデータ取引管理制度を構築、健全化し、データ取引行為を規範化し、データ取引市場を育成する。

第十八条 国は大学・大学院、職業学校と企業などがデータの開発利用技術と安全に係る教育と研修を展開することをサポートし、様々な方式を採用してデータ開発利用技術と安全に係る専門人材を養成し、人材の交流を促進する。

### 第三章 データ安全制度

第十九条 国はデータが経済社会発展中の重要度によって、またはいったん改ざん、破壊、漏洩或は不法取得、不法利用された場合、国の安全、公共の利益或は公民、組織の合法的な權益への危害の程度によって、データに対してランク付け、分類し保護する。

各地区、各部門は、国の関連規定に基づいて、本地区、本部門、本業界の重要データ保護目録を確定し、目録に登録されたデータを重点的に保護する。

第二十条 国は集中且つ統一、高効率、権威的なデータ安全リスク評価、報告、情報共有、モニタリング・警報メカニズムを構築し、データ安全に係るリスク情報の取得、分析、研究・判断、警報を強化する。

第二十一条 国はデータの安全に係る緊急対応メカニズムを構築する。

データの安全に係る事件が発生した場合、関連主管部門は法律に基づいて緊急計画を始動し、相応の緊急対応措置をとらなければならない。安全の潜在的リスクを取り除き、危害の拡大を防止し、且つ公衆に関係のある警告情報を遅滞なく社会に対し発表しなければならない。

第二十二条 国はデータ安全審査制度を構築し、国の安全に影響を与える、または影響を与える可能性のあるデータ活動について、国の安全審査を実施する。

法律に基づいた安全審査の判断が最終決定となる。

第二十三条 国は、国際的義務の履行や国の安全保障の維持に関連する規制対象品目に該当するデータについて、法律に基づいて輸出規制を実施する。

第二十四条 いかなる国あるいは地域も、データ及びデータの開発利用技術などに係る投資、貿易面にお

いて中華人民共和国に対して差別的な禁止、制限又はその他の類似する措置を講じた場合、中華人民共和国は、実情に応じて、当該国あるいは地域に対して相応した措置を講ずることができる。

#### 第四章 データの安全保護義務

第二十五条 データ活動を展開する際は、法律、行政法規の規定と国家標準の強制的要求に従い、全プロセスのデータセキュリティ管理制度を構築、健全化し、データセキュリティ教育研修を実施し、関連技術措置及びその他の必要な措置を取り、データの安全を保障しなければならない。

重要データの処理者は、データセキュリティの責任者と管理機構を設け、データの安全保護の責任を確実に明確にしなければならない。

第二十六条 データ活動の展開、データに係る新技術の研究・開発は、経済社会の発展を促進し、国民の福祉を増進させ、社会の公衆道徳に合致するものでなければならない。

第二十七条 データ活動を展開する際は、リスクモニタリングを強化しなければならない。データセキュリティの欠陥やセキュリティホールなどのリスクが発見された場合は、直ちに是正措置を講じなければならない。データの安全に係る事件が発生した場合は、規定に基づいて、速やかに使用者に通知し、同時に関連主管部門に送付・報告しなければならない。

第二十八条 重要データの処理者は、規定に基づいて、データ活動について定期的にリスク評価を実施し、関連主管部門にリスク評価レポートを送付・報告しなければならない。

リスク評価レポートには、当該組織が把握している重要データの種類と量、データの収集、保存、加工、使用状況、データセキュリティリスクとその対処方法などが含まなければならない。

第二十九条 いかなる組織や個人もデータを収集する際は、合法的かつ正当な手段を使わなければならない。窃盗など不法な方法でデータを取得してはならない。

法律、行政法規が、データの収集、利用の目的、範囲について規定している場合は、法律、行政法規の規定範囲内で、データを収集し、利用しなければならない。必要な限度を超えてはならない。

第三十条 データ取引仲介サービスを提供する事業者が取引仲介サービスを提供する際は、データの提供者にデータのソースを説明してもらい、取引双方の身元を確認し、かつその確認記録と取引記録を保存しなければならない。

第三十一条 オンラインデータ処理等のサービスを提供する事業者は、法に基づいて経営許可の取得もしくは届出をしなければならない。具体的な方法は国务院の電信主管部門が関連部署と共同で制定する。

第三十二条 公安機関、国家安全機関が、法に基づいて国の安全を保護し、または犯罪を捜査する際に、データを取寄せ必要がある場合は、国の関連規定に基づき、厳格な承認プロセスを経て、法に基づいて行わなければならない。関連組織や個人は、これに協力しなければならない。



第三十三条 国外の法執行機関が、中華人民共和国国内に保存されたデータを取寄せる際は、関連組織や個人が関連主管機関に報告し、許可を得た後、提供しなければならない。中華人民共和国が締結または参加している国際条約、協定で、国外の法執行機関によるデータ取寄せについて規定がある場合は、その規定に従わなければならない。

## 第五章 政務関連データの安全と公開

第三十四条 政務の電子化を推進し、政務関連データの科学性、正確性、時効性を高め、データの運用を通じて経済社会の発展に貢献する能力を向上させる。

第三十五条 国の機関が法の定める職責を履行するために、データを収集し使用する場合は、その法の定める職責の範囲内で、法律、行政法規で定められた条件とプロセスに従って、行わなければならない。

第三十六条 国の機関は法律、行政法規の規定に基づいて、データの安全管理制度を構築、健全化し、データの安全に係る保護責任を確実に明確にし、政務関連データの安全を保証しなければならない。

第三十七条 国の機関が第三者に、政務関連データの保存、加工を依頼し、あるいは第三者にデータを提供する場合は、厳格な承認プロセスを経て、かつデータの受取側が適切なデータの安全に係る保護義務を果たすことを、監督しなければならない。

第三十八条 国の機関は公正、公平、民衆の便利性の原則に基づき、規定に基づいて、政務関連データを遅滞なく、かつ正確に公開しなければならない。法に基づき非公開とする場合を除く。

第三十九条 国は政務関連データの公開目録を制定し、政務関連データの統一的・規範化され、相互アクセス可能で、安全で制御可能な公開プラットフォームを構築し、政務関連データの開放・利用を推進する。

第四十条 公共事務の管理機能を持つ組織が、公共事務の管理機能を履行するために、データ活動を展開する場合は、本章の規定が適用される。

## 第六章 法的責任

第四十一条 関連主管部門は、データの安全監督管理の職責の履行において、データ活動に比較的大きな安全に係るリスクが存在することを発見した場合には、規定に基づいた権限及びプロセスに従い、関連組織と個人に対し事情聴取を行うことができる。関連組織と個人は、要求に従い措置を講じて是正し、潜在的リスクを取り除かなければならない。

第四十二条 データ活動を展開する組織、個人が本法第二十五条、第二十七条、第二十八条、第二十九条にて定められたデータの安全に係る保護義務を履行していない、あるいは必要な安全措置を講じていない場合には、関係主管部門が是正するよう命じ、警告するとし、且つ1万元以上10万元以下の罰金を科

すこともでき、また直接の責任を負う主管者に対し5,000元以上5万元以下の罰金を科すことができる。是正を拒否する、あるいは大量のデータ漏洩などの重大な結果をもたらした場合には、10万元以上100万元以下の罰金を科し、直接の責任を負う主管者とその他の直接責任のある者に対して1万元以上10万元以下の罰金を科す。

第四十三条 データ取引仲介機構が本法第三十条に定める義務を履行しなかったことにより、不法な方式で取得したデータによる取引につながった場合には、関連主管部門が是正を命じ、違法所得を没収し、且つ違法所得の倍以上十倍以下の罰金を科す。違法所得がない場合には、10万元以上100万元以下の罰金を科し、且つ関係主管部門が関連業務許可証、又は営業許可証の取消しを命ずることができる。直接の責任を負う主管者とその他の直接責任のある者に対して1万元以上10万元以下の罰金を科す。

第四十四条 許可又は届出を取得せず、無断で本法第三十一条にて定める業務に従事した場合には、関連主管部門は是正を命じ又は取締り、違法所得を没収し、且つ違法所得の倍以上十倍以下の罰金を科す。違法所得がない場合には、10万元以上100万元以下の罰金を科す。直接の責任を負う主管者とその他の直接責任のある者に対して1万元以上10万元以下の罰金を科す。

第四十五条 国の機関が本法にて定めるデータの安全に係る保護義務を履行していない場合、直接の責任を負う主管者とその他の直接責任のある者に対して、法に基づいて処分する。

第四十六条 データの安全に係る監督責任を履行する職員が職務懈怠、職権濫用、私利をはかったものの、犯罪には至らなかった場合、法に基づいて処分する。

第四十七条 データ活動によって国の安全、公共利益に危害を与える、又は公民、組織の合法的な權益に損害をもたらした場合、関連法律、行政法規に基づいて処罰する。

第四十八条 本法の規定に違反し、他人に損害をもたらした場合には、法に基づいて民事責任を負う。本法の規定に違反し、治安管理条例違反行為に至る場合には、法に基づいて治安管理条例に係る処分を行う。犯罪に至る場合には、法に基づいて刑事責任を追及する。

## 第七章 附則

第四十九条 国の秘密に関わるデータ活動については、『中華人民共和国国家秘密保守法』などの法律や行政法規の規定が適用される。個人情報に係るデータ活動を展開する場合には、法律、行政法規の規定に従う。

第五十条 軍事に関わるデータ安全の保護については、中央軍事委員会が、これを別途定める。

第五十一条 本法は 年 月 日から施行される。

## 中华人民共和国数据安全法(草案)

### 目 录

#### 第一章 总 则

#### 第二章 数据安全与发展

#### 第三章 数据安全制度

#### 第四章 数据安全保护义务

#### 第五章 政务数据安全与开放

#### 第六章 法律责任

#### 第七章 附 则

#### 第一章 总 则

第一条 为了保障数据安全,促进数据开发利用,保护公民、组织的合法权益,维护国家主权、安全和发展利益,制定本法。

第二条 在中华人民共和国境内开展数据活动,适用本法。

中华人民共和国境外的组织、个人开展数据活动,损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的,依法追究法律责任。

第三条 本法所称数据,是指任何以电子或者非电子形式对信息的记录。

数据活动,是指数据的收集、存储、加工、使用、提供、交易、公开等行为。

数据安全,是指通过采取必要措施,保障数据得到有效保护和合法利用,并持续处于安全状态的能力。

第四条 维护数据安全,应当坚持总体国家安全观,建立健全数据安全治理体系,提高数据安全保障能力。

第五条 国家保护公民、组织与数据有关的权益,鼓励数据依法合理有效利用,保障数据依法有序自由流动,促进以数据为关键要素的数字经济发展,增进人民福祉。

第六条 中央国家安全领导机构负责数据安全工作的决策和统筹协调,研究制定、指导实施国家数据安全战略和有关重大方针政策。

第七条 各地区、各部门对本地区、本部门工作中产生、汇总、加工的数据及数据安全负主体责任。

工业、电信、自然资源、卫生健康、教育、国防科技工业、金融业等行业主管部门承担本行业、本领域数据安全监管职责。

公安机关、国家安全机关等依照本法和有关法律、行政法规的规定,在各自职责范围内承担数据安全监管

职责。

国家网信部门依照本法和有关法律、行政法规的规定,负责统筹协调网络数据安全和相关监管工作。

第八条 开展数据活动,必须遵守法律、行政法规,尊重社会公德和伦理,遵守商业道德,诚实守信,履行数据安全保护义务,承担社会责任,不得危害国家安全、公共利益,不得损害公民、组织的合法权益。

第九条 国家建立健全数据安全协同治理体系,推动有关部门、行业组织、企业、个人等共同参与数据安全保护工作,形成全社会共同维护数据安全和促进发展的良好环境。

第十条 国家积极开展数据领域国际交流与合作,参与数据安全相关国际规则和标准的制定,促进数据跨境安全、自由流动。

第十一条 任何组织、个人都有权对违反本法规定的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。

## 第二章 数据安全与发展

第十二条 国家坚持维护数据安全和促进数据开发利用并重,以数据开发利用和产业发展促进数据安全,以数据安全保障数据开发利用和产业发展。

第十三条 国家实施大数据战略,推进数据基础设施建设,鼓励和支持数据在各行业、各领域的创新应用,促进数字经济发展。

省级以上人民政府应当制定数字经济发展规划,并纳入本级国民经济和社会发展规划。

第十四条 国家加强数据开发利用技术基础研究,支持数据开发利用和数据安全等领域的技术推广和商业创新,培育、发展数据开发利用和数据安全产品和产业体系。

第十五条 国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责,组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、研究机构、高等学校、相关行业组织等参与标准制定。

第十六条 国家促进数据安全检测评估、认证等服务的发展,支持数据安全检测评估、认证等专业机构依法开展服务活动。

第十七条 国家建立健全数据交易管理制度,规范数据交易行为,培育数据交易市场。

第十八条 国家支持高等学校、中等职业学校和企业等开展数据开发利用技术和数据安全相关教育和培训,

采取多种方式培养数据开发利用技术和数据安全专业人才,促进人才交流。

### 第三章 数据安全制度

第十九条 国家根据数据在经济社会发展中的重要程度,以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用,对国家安全、公共利益或者公民、组织合法权益造成的危害程度,对数据实行分级分类保护。

各地区、各部门应当按照国家有关规定,确定本地区、本部门、本行业重要数据保护目录,对列入目录的数据进行重点保护。

第二十条 国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制,加强数据安全风险信息的获取、分析、研判、预警工作。

第二十一条 国家建立数据安全应急处置机制。

发生数据安全事件,有关主管部门应当依法启动应急预案,采取相应的应急处置措施,消除安全隐患,防止危害扩大,并及时向社会发布与公众有关的警示信息。

第二十二条 国家建立数据安全审查制度,对影响或者可能影响国家安全的数据活动进行国家安全审查。依法作出的安全审查决定为最终决定。

第二十三条 国家对与履行国际义务和维护国家安全相关的属于管制物项的数据依法实施出口管制。

第二十四条 任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的,中华人民共和国可以根据实际情况对该国家或者地区采取相应的措施。

### 第四章 数据安全保护义务

第二十五条 开展数据活动应当依照法律、行政法规的规定和国家标准的强制性要求,建立健全全流程数据安全管理制度,组织开展数据安全教育培训,采取相应的技术措施和其他必要措施,保障数据安全。

重要数据的处理者应当设立数据安全负责人和管理机构,落实数据安全保护责任。

第二十六条 开展数据活动以及研究开发数据新技术,应当有利于促进经济社会发展,增进人民福祉,符合社会公德和伦理。

第二十七条 开展数据活动应当加强风险监测,发现数据安全缺陷、漏洞等风险时,应当立即采取补救措施;发生数据安全事件时,应当按照规定及时告知用户并向有关主管部门报告。

第二十八条 重要数据的处理者应当按照规定对其数据活动定期开展风险评估,并向有关主管部门报送风



险评估报告。

风险评估报告应当包括本组织掌握的重要数据的种类、数量,收集、存储、加工、使用数据的情况,面临的数据安全风险及其应对措施等。

第二十九条 任何组织、个人收集数据,必须采取合法、正当的方式,不得窃取或者以其他非法方式获取数据。

法律、行政法规对收集、使用数据的目的、范围有规定的,应当在法律、行政法规规定的目的和范围内收集、使用数据,不得超过必要的限度。

第三十条 从事数据交易中介服务的机构在提供交易中介服务时,应当要求数据提供方说明数据来源,审核交易双方的身份,并留存审核、交易记录。

第三十一条 专门提供在线数据处理等服务的经营者,应当依法取得经营业务许可或者备案。具体办法由国务院电信主管部门会同有关部门制定。

第三十二条 公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据,应当按照国家有关规定,经过严格的批准手续,依法进行,有关组织、个人应当予以配合。

第三十三条 境外执法机构要求调取存储于中华人民共和国境内的数据的,有关组织、个人应当向有关主管机关报告,获得批准后方可提供。中华人民共和国缔结或者参加的国际条约、协定对外国执法机构调取境内数据有规定的,依照其规定。

## 第五章 政务数据安全与开放

第三十四条 国家大力推进电子政务建设,提高政务数据的科学性、准确性、时效性,提升运用数据服务经济社会发展的能力。

第三十五条 国家机关为履行法定职责的需要收集、使用数据,应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行。

第三十六条 国家机关应当依照法律、行政法规的规定,建立健全数据安全管理制度,落实数据安全保护责任,保障政务数据安全。

第三十七条 国家机关委托他人存储、加工政务数据,或者向他人提供政务数据,应当经过严格的批准程序,并应当监督接收方履行相应的数据安全保护义务。

第三十八条 国家机关应当遵循公正、公平、便民的原则,按照规定及时、准确地公开政务数据。依法不

予公开的除外。

第三十九条 国家制定政务数据开放目录,构建统一规范、互联互通、安全可控的政务数据开放平台,推动政务数据开放利用。

第四十条 具有公共事务管理职能的组织为履行公共事务管理职能开展数据活动,适用本章规定。

## 第六章 法律责任

第四十一条 有关主管部门在履行数据安全监管职责中,发现数据活动存在较大安全风险的,可以按照规定的权限和程序对有关组织和个人进行约谈。有关组织和个人应当按照要求采取措施,进行整改,消除隐患。

第四十二条 开展数据活动的组织、个人不履行本法第二十五条、第二十七条、第二十八条、第二十九条规定的数据安全保护义务或者未采取必要的安全措施的,由有关主管部门责令改正,给予警告,可以并处一万元以上十万元以下罚款,对直接负责的主管人员可以处五千元以上五万元以下罚款;拒不改正或者造成大量数据泄漏等严重后果的,处十万元以上一百万元以下罚款,对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第四十三条 数据交易中介机构未履行本法第三十条规定的义务,导致非法来源数据交易的,由有关主管部门责令改正,没收违法所得,处违法所得一倍以上十倍以下罚款,没有违法所得的,处十万元以上一百万元以下罚款,并可以由有关主管部门吊销相关业务许可证或者吊销营业执照;对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第四十四条 未取得许可或者备案,擅自从事本法第三十一条规定业务的,由有关主管部门责令改正或者予以取缔,没收违法所得,处违法所得一倍以上十倍以下罚款;没有违法所得的,处十万元以上一百万元以下罚款;对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第四十五条 国家机关不履行本法规定的数据安全保护义务的,对直接负责的主管人员和其他直接责任人员依法给予处分。

第四十六条 履行数据安全监管责任的国家工作人员玩忽职守、滥用职权、徇私舞弊,尚不构成犯罪的,依法给予处分。

第四十七条 通过数据活动危害国家安全、公共利益,或者损害公民、组织合法权益的,依照有关法律、行政法规的规定处罚。

第四十八条 违反本法规定,给他人造成损害的,依法承担民事责任。违反本法规定,构成违反治安管理处

罚行为的,依法给予治安管理处罚;构成犯罪的,依法追究刑事责任。

## 第七章 附 则

第四十九条 涉及国家秘密的数据活动,适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。开展涉及个人信息的数据活动,应当遵守有关法律、行政法规的规定。

第五十条 军事数据安全保护的办 法,由中央军事委员会另行制定。

第五十一条 本法自 年 月 日起施行。

以上

### 【照会先】

担当者：中国アドバイザー一部・総括チーム 張巍

Tel : 021-3855-8888 (Ext : 1185)

E-mail : [uei.zhang@mizuho-cb.com](mailto:uei.zhang@mizuho-cb.com)

政策の適用にあたり、具体的な実務手続き等については、所在地の主管部門または法律事務所等にお問い合わせください。

本ビジネス・エクスプレスは原則、週次を目途に発行しております。

Copyright © 2020 Mizuho Bank (China), Ltd

1. 本件記載の情報は、法律上・会計上・税務上の助言を含むものではありません。法律上・会計上・税務上の助言を必要とされる場合には、それぞれの専門家にご相談ください。
2. 本件記載の情報の開示は貴社の守秘義務を前提とするものです。当該情報については貴社内部の利用に限定され、その内容の第三者への開示は禁止されています。
3. 本件記載の著作権は原則として弊行に帰属します。いかなる目的であれ本件の一部または全部について無断で、いかなる方法においても複写・複製・引用・転載・翻訳・貸与等を行うことを禁止します。
4. 本件記載の情報は、弊行が信頼できると考える各方面から取得しておりますが、その内容の正確性・信頼性・完全性を保証するものではありません。弊行は当該情報に起因して発生した損害については、その内容如何にかかわらず一切責任を負いません。